DISPUTES MANAGEMENT

Best practices to help avoid chargebacks/ disputes

September 2023

globalpayments

To help minimize losses, you need an adequate **chargeback tracking system and procedures** in place to avoid unnecessary chargebacks and have a thorough understanding of your rights.

We've prepared this document as a reference to follow best practices to mitigate and manage chargebacks:

- **Do not complete a transaction if the authorization request was declined**. Do not repeat the authorization request after receiving a decline; ask for another form of payment.
- **Show good customer service**
    - If the merchandise or service to be provided to the customer will be delayed, advise the customer in writing of the delay and the new expected delivery or service date.
    - If the customer has ordered merchandise that is out of stock or no longer available, advise the customer in writing. If the merchandise is out of stock, let the customer know when it will be delivered. If an item is no longer available, offer the option of either purchasing a similar item or cancelling the transaction. Do not substitute another item unless the customer agrees to accept it.
    - If a customer requests cancellation of a transaction that is billed periodically (monthly, quarterly, or annually), cancel the transaction immediately or as specified by the customer. Also advise the customer in writing that the service, subscription, or membership has been cancelled and state the effective date of the cancellation.
- **Ship merchandise before depositing transactions**. For card-not-present transactions, do not deposit transaction receipts with your acquirer until you have shipped the related merchandise. If customers see the transaction on their monthly card statement before they receive the merchandise, they may contact their issuer to dispute the billing. Similarly, if delivery is delayed on a

card-present transaction, do not deposit the transaction receipt until the merchandise has been shipped.

- **Have clear terms and conditions**. For card-not-present transactions, publish clear terms and conditions, including your return policy. If product returns are not permitted, state that clearly.
- **Confirm delivery for all shipments**. Require signature for deliveries. To prevent chargebacks involving cardholder service/merchandise not being received especially during the holiday season, it is highly suggested that merchants require signatures for deliveries.
- **Act promptly when customers with valid disputes deserve credits.**
    - When cardholders contact you directly to resolve a dispute, issue the credit on a timely basis to avoid unnecessary disputes and their associated chargeback processing costs.
    - Send cardholders an email message to let them know immediately of the impending credit.
- **Provide data-rich responses to sales draft requests**.
    - Response in a timely manner to sales draft inquiries from your acquirer with full information about the sale, and be sure to include the following required data elements:
        - Account number
        - Card expiration date
        - Cardholder name
        - Transaction date
        - Transaction amount
        - Authorization code
        - Merchant name
        - Merchant online address
        - General description of goods or services
        - "Ship to" address, if applicable
        - Transaction time
        - Customer email address
        - Customer telephone number
        - Customer billing address
        - Detailed description of goods or services
        - Customer login or user ID
        - Customer IP address
        - Customer device ID or device fingerprint
        - Whether a receipt signature was obtained upon delivery of goods or services
        - Use clear billing descriptors so customers can easily identify their purchase on their monthly bank statements, reducing any confusion that may lead to a dispute.

Best practices for ecommerce processing and reversing authorization

This article provides recommended processing for authorization, authorization reversal, and clearing when dealing with estimated amounts and multi-item purchases where all items may or may not be delivered or are not delivered at the same time. These best practices are intended to help guide dual message acquirers, issuers, and processors in the usage of these transactions.

Background
Ecommerce authorizations are intended to reserve funds for subsequent clearing transactions once online purchases are dispatched (for example, physical items shipped or electronic content delivered). The information below may also be applied to mail order/telephone order (MOTO) (non-T&E) transactions.

Guiding principles
The following is provided as guidance for ecommerce processing. Note that unless otherwise specified, these are best practices and not mandatory:

- An approved ecommerce authorization will have only one first presentment unless multi-clearing processing is utilized with the proper message reason codes indicating that the issuer should maintain hold of funds for subsequent presentments.

  Note:
  As specified in the chargeback guide, airline ticket and installment purchases are allowed multiple first presentments against one approved authorization.

- Mastercard recommends that merchants submit reversals once an adjustment to the original authorization amount is known.

  Note:
  1. You must submit a full or partial reversal (as applicable) within seven (7) calendar days of an original undefined authorization or final authorization request, and within thirty (30) calendar days of an original preauthorization request.
  2. You must submit a full or partial reversal within 24 hours of transaction cancellation or of the transaction completing for an amount different from the authorized amount.

- Issuers must release any hold of funds once a clearing presentment has been matched (using the Trace ID amongst other data elements) to the original ecommerce authorization unless multi-clearing processing is utilized.

- If an ecommerce item ships late (beyond the authorization expiration date), you may submit a chargeback extension request message to avoid chargeback for message reason code 4808—Requested/Required Authorization Not Obtained. If the issuer approves the extension request, you will be protected from chargeback reason 4808 as long as the item ships prior to the new authorization expiration date.

- If an ecommerce item ships late and you have not requested or did not receive approval of a chargeback period extension request and the authorization chargeback protection period has expired, you must submit a new authorization for the item to be shipped to avoid chargeback message reason code 4808—Requested/Required Authorization Not Obtained. The new authorization will take on the security characteristics of the original authorization within a dispute resolution.

  Note:
  1. The best practice for extending the payment guarantee and avoiding a chargeback is to submit an incremental authorization to refresh the authorization date. In the Europe region currently, a nominal amount (such as an amount of USD 0.00) should be used instead.
  2. Without Universal Cardholder Authentication Field (UCAF™) data present, a re-authorized transaction must be presented within clearing for non-UCAF interchange (as applicable by region).

Authorization dos and don'ts

This segment summarizes dos and don’ts for ecommerce businesses when obtaining authorization for card-not-present transactions, in order to help prevent potential disputes and violations of proper transaction processing.

- If you are unable to determine the final transaction amount because sales tax and/or shipping cost is not known at the time of purchase:

- **Do**: Authorize for the anticipated transaction amount without sales tax and/or shipping cost. If the clearing amount (transaction amount + shipping + tax) is within 15% variance between the original authorization amount and the clearing amount, then clear the transaction amount plus sales tax and shipping amount. If the clearing amount (transaction amount + shipping + tax) is greater than a 15% variance between the authorization amount and the clearing amount, clear the original transaction amount as shipped and then authorize and create a new transaction for the additional amount that is above the original authorization amount.
- **Don't**: Clear a single final transaction amount that is greater than 15% of the authorization amount due to tax and shipping. This can result in a rule violation and chargeback exposure.

- When processing a single purchase into multiple shipments:
  - **Do**: Authorize the total purchase amount. For each shipment within seven (7) calendar days of authorization, clear each shipment amount as each item is shipped and include the following fields:
    - Original authorization transaction ID
    - Original authorization code
    - Authorized amount
    - Total authorized amount = authorization less amount reversed
    - Multiple clearing sequence number
    - Multiple clearing sequence count
  - **Don't**: Clear multiple shipments using original authorization without the Multiple Clearing Sequence Number/Count and/or without the original authorization transaction ID and authorization code. This can result in CPS downgrade, rules violation, processing integrity fees, and global duplicate transaction ID fees. Also, do not clear multiple shipments using the original authorization without including the authorized amount and total authorized amount fields in the clearing transactions. This can result in a CPS downgrade.
- If you or the customer cancels the order prior to shipment:
  - **Do**: Authorize for the total purchase amount and reverse the original authorization (within 72 hours).
  - **Don't**: Authorize for the total purchase amount, and not reverse original authorization. This can result in processing integrity fees and/or a rules violation.
- If the order amount is adjusted prior to final shipment:
  - **Do**: Authorize for the original purchase amount. For shipment amounts < original authorization:
    - If a shipment is within seven (7) calendar days of authorization, partially reverse the difference between the authorized amount and the shipment amount, then clear the shipment amount as shipped.
    - If a shipment is after seven (7) calendar days of authorization, first reverse the original authorization within three (3) days. Then authorize the new amount and clear the shipment amount as shipped.
  - **Don't**: Clear the final transaction more than seven (7) calendar days from the original authorization date. This can result in a rule violation and chargeback exposure.

3D Secure

Process

The following provides a basic understanding of the 3D Secure process. These best practices are intended to help guide dual message acquirers, issuers, and processors in using these transactions.

Background
3D Secure is a global standard on cardholder authentication developed by payment networks for electronic commerce transactions. Visa branded their implementation Visa 3D Secure and Mastercard branded theirs SecureCode.

3D Secure is a global ecommerce solution that enables cardholders to authenticate themselves to their card issuer by using a unique personal code. Mastercard SecureCode and Visa 3D Secure address current concerns about the security of online shopping and the high rate of ecommerce chargebacks. They're designed to take online shopping and consumer confidence to a new level.

Both SecureCode and Visa 3D Secure require 3D Secure technology to be deployed on your website. This can be done by loading a payment network registered Merchant Plug-In (MPI) application on your server. Alternatively, you can contract with a hosted service to perform the authentication process for you.

The 3D Secure transaction cycle is composed of enrollment, authentication and authorization. In the enrollment phase, once the item is checked out, you request the issuer to verify if the cardholder is enrolled in the Mastercard SecureCode/Visa 3D Secure service. It will then be authenticated to verify the identity of the cardholder prior to the transaction taking place. Then authorization will be requested to prove the successful authentication of the cardholder.

3D Secure is designed to help online merchants:

- Reduce fraud
- Reduce chargebacks
- Increase online business
- Increase cardholder confidence

Process flow

1. The cardholder enters their card details on the checkout page.
2. Your MPI (Merchant Plug-In) contacts either the Mastercard or Visa directory to check for the card issuers' participation.
3. The directory responds either "Yes" (go to next step) or "No" (go to step 6).
4. If the payment network chooses to authenticate the cardholder, a space appears on your website for the cardholder to input their unique password or enroll during shopping (go to the next step). If the payment network chooses not to authenticate the cardholder, go to step 6.
5. The payment network validates the unique password and sends an authentication response back to your MPI.
6. Your system then requests authorization in the usual way, but containing the additional authentication data.

Note:
If a registered cardholder's identification details are not approved, you shouldn't continue with the transaction. Your normal operational practices should then determine how you proceed, which may include asking for an alternative means of payment instead.

Best practices

The following is provided as guidance for the 3D Secure liability shift and sample case scenario. The following guidelines help you address the chargeback filed against your business.

Understand the Visa 3D Secure or Mastercard SecureCode liability shift rules. Visa 3D Secure or SecureCode participating merchants are protected by their acquirer from receiving certain fraud-related chargebacks only, provided the transaction is processed correctly.

If:	Ecommerce / UCAF indicator	Chargeback protection
Both the Issuer and Acquirer are secured	2 – For Mastercard 5 – For Visa	Protected under fraud-related chargeback.
The card issuer or cardholder is not participating in Visa 3D Secure or Mastercard SecureCode	1 – For Mastercard 6 – For Visa	Protected under fraud-related chargeback.
The card issuer is unable to authenticate	0 – For Mastercard 7 – Visa	No protection against fraud

Note:
If you are enrolled in Visa 3D Secure and Mastercard SecureCode, refer to the payment authentication search in MIGS or CyberSource to check for security level.

Sample case scenario
The following is provided as a sample illustration of how the chargeback/dispute will be resolved involving 3D Secure transactions.

Case Scenario 1

Q. The merchant claims that the transaction was processed as 3D Secure however per checking in card brand records, the transaction is ECI 7 or MOTO 1.

A. Unfortunately, we are unable to defend this case as this transaction was not authorized as 3D Secure. As advised in the card processing guide, card-not-present transactions are taken at your own risk.

Case Scenario 2

Q. The transaction is ECI 6 however the CAVV is 0 or blank.

A. Although the transaction appears to be 3D Secure, the merchant needs to provide Payer Authentication Request (PAREQ), Payer Authentication Response (PARES), Verify Enrollment Response (VERES) and details of the CAVV to confirm full authentication was obtained.

Case scenario 3

Q. The transaction is authorized as ECI 5 however the clearing record shows ECI 7.

A. Unfortunately, we are unable to defend this case as this transaction was not authorized as 3D Secure. As advised in the card processing guide, card-not-present transactions are taken at your own risk.

We're here to help Our cloud-based productivity and performance tools—combined with our expert insight and guidance—help you build your business, whatever stage you're at.

Please call us at +1 800 361-8170

Or learn more at globalpayments.com/en-ca

Disclaimer

Global Payments is not responsible for use of information contained in this document (including errors, omissions, or inaccuracy of any kind) or any assumptions or conclusions you might draw from its use. No warranty or representation is given to the completeness or otherwise of this information. It is being provided to share best practices which Global Payments deems helpful for managing chargebacks.

globalpayments Innovation that delivers.